The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
12/08/2020

SUBJECT:
A Vulnerability in Apache Struts Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in Apache Struts, which could allow for remote code execution. Apache Struts is an open source framework used for building Java web applications. Successful exploitation of this vulnerability could allow for remote code execution. Depending on the privileges associated with the user, an attacker could then install programs; view; change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- Apache Structs versions prior to 2.5.26

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Apache Struts, which could allow for remote code execution. This vulnerability exists due to some of the tag attributes performing a double evaluation if a developer applied forced OGNL evaluation by using the %{…} syntax. Using forced OGNL evaluation on untrusted user input can lead to remote code execution and security degradation. Successful exploitation of this vulnerability could allow for remote code execution.

Depending on the privileges associated with the user, an attacker could then install programs; view; change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Upgrade to the most recent version of Apache Struts after appropriate testing.
- Verify no unauthorized system modifications have occurred on the system before applying the patch.
- Frequently validate type and content of uploaded data.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:
Apache:
https://cwiki.apache.org/confluence/display/WW/S2-061Link 2

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17530

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/